

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-321750

(43)Date of publication of application : 12.12.1997

(51)Int.Cl.

H04L 9/34
H04H 1/02
H04K 1/06
H04N 7/167

(21)Application number : 08-328617

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 09.12.1996

(72)Inventor : SHIROSHITA TERUJI

(30)Priority

Priority number : 07320903
08 77602

Priority date : 08.12.1995
29.03.1996

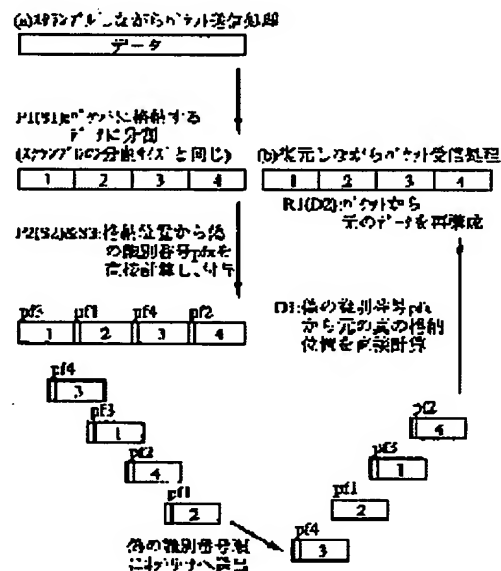
Priority country : JP
JP

(54) SCRAMBLE COMMUNICATION METHOD AND SYSTEM THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To reduce processing amount and processing time which are necessary for scrambling processing and restore processing by dividing data into plural data units being a packet size, giving a false packet identifier which indicates scrambled packet order, assembling a packet and executing transmission to a network by means of the packet order which is scrambled based on the false packet identifier.

SOLUTION: Whole data is scrambled and divided into a proper packet size in packet transmission with scrambling (P1(S1)). A false packet identifying number pfx is directly calculated from the memory address of division data in the respective packets so as to be given to the respective packets and, while executing this, the packet is assembled. (P2(S2) and S3). In the meantime, in packet reception while executing restoration, the packet is received while directly calculating the memory address of division data from the false packet identifying number pfx(D1). Then, whole original data is re-constituted based on the memory address of division data (R1(D2)).



LEGAL STATUS

[Date of request for examination]

13.12.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-321750

(43) 公開日 平成9年(1997)12月12日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/34			H 0 4 L 9/00	6 8 1
H 0 4 H 1/02			H 0 4 H 1/02	E
H 0 4 K 1/06			H 0 4 K 1/06	
H 0 4 N 7/167			H 0 4 N 7/167	Z

審査請求 未請求 請求項の数20 O L (全 18 頁)

(21) 出願番号 特願平8-328617

(22) 出願日 平成8年(1996)12月9日

(31) 優先権主張番号 特願平7-320903

(32) 優先日 平7(1995)12月8日

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願平8-77602

(32) 優先日 平8(1996)3月29日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 城下 輝治

東京都新宿区西新宿三丁目19番2号 日本

電信電話株式会社内

(74) 代理人 弁理士 三好 秀和 (外1名)

(54) 【発明の名称】 スクランブル通信方法及びシステム

(57) 【要約】

【課題】 送信側や受信側におけるスクランブル処理や復元処理に必要な処理量や処理時間を軽減することが可能なスクランブル通信方法及びシステムを提供すること。

【解決手段】 送信側においては、元のデータをパケットサイズの複数のデータ単位に分割し、データ単位をパケットに格納して該パケットにスクランブルしたパケット順序を示す偽のパケット識別子を付与して該パケットを組み立て、パケットを偽のパケット識別子に基づいてスクランブルしたパケット順序でネットワークに送信することにより、元のデータをスクランブルする。受信側においては、偽のパケット識別子から真のデータ単位順序を示すデータ単位順序情報を復元し、パケットに格納されたデータ単位から該データ単位順序情報に基づいて元のデータを再構成することにより、ネットワークから受信した前記パケットを復元する。

(a) スクランブルしながらパケット送信処理

データ

P1(S1): パケットに格納する
データに分割
(スランブルの分割単位と同じ)

1 2 3 4

P2(S2): パケットの組立

S3: 偽の識別番号pf_xに置き換え

pf₃ pf₁ pf₄ pf₂
1 2 3 4

pf₄ 3
pf₃ 1
pf₂ 4
pf₁ 2
偽の識別番号順
にネットワークへ送出
pf₄ 3

(b) 復元しながらパケット受信処理

1 2 3 4
p₁ p₂ p₃ p₄

R1(D2): パケットから元の
データを再構成

D1: 真の識別番号に
戻しながら受信

pf₂ 4
pf₃ 1
pf₁ 2
pf₄ 3

【特許請求の範囲】

【請求項1】 ネットワークで接続された送信側と受信側間のスクランブル通信方法であって、送信側において、元のデータをバケットサイズの複数のデータ単位に分割し、該データ単位をバケットに格納して該バケットにスクランブルしたバケット順序を示す偽のバケット識別子を付与して該バケットを組み立て、該バケットを該偽のバケット識別子に基づいてスクランブルしたバケット順序でネットワークに送信することにより、該元のデータをスクランブルするステップと、
 10 受信側において、前記偽のバケット識別子から真のデータ単位順序を示すデータ単位順序情報を復元し、前記バケットに格納された前記データ単位から該データ単位順序情報に基づいて前記元のデータを再構成することにより、ネットワークから受信した前記バケットを復元するステップと、
 を有することを特徴とするスクランブル通信方法。

【請求項2】 前記スクランブルするステップは、スクランブルされていないバケット順序を示す真のバケット識別子を前記バケットに付与し、所定のスクランブルキーに基づいて該真のバケット識別子を前記偽のバケット識別子に置き換えることにより該バケットを組み立て、前記復元するステップは、前記所定のスクランブルキーに対応する所定のアセンブルキーに基づいて前記偽のバケット識別子を前記真のバケット識別子に変換し、前記元のデータを再構成するにあたって該真のバケット識別子を前記データ単位順序情報として用いることにより該データ単位順序情報を復元する、
 20 ことを特徴とする請求項1記載のスクランブル通信方法。

【請求項3】 前記スクランブルするステップは、所定の計算手順に基づいて前記データ単位のメモリアドレスから前記偽のバケット識別子を直接計算して前記バケットを組み立て、前記復元するステップは、所定の計算手順に基づいて前記偽バケット識別子から前記データ単位のメモリアドレスを直接計算し、前記元のデータを再構成するにあたって該メモリアドレスを前記データ単位順序情報として用いることにより該データ単位順序情報を復元する、
 30 ことを特徴とする請求項1記載のスクランブル通信方法。

【請求項4】 前記スクランブルするステップは、送信側におけるプロトコル処理により行われることを特徴とする請求項1記載のスクランブル通信方法。

【請求項5】 前記復元するステップは、受信側におけるプロトコル処理により行われることを特徴とする請求項1記載のスクランブル通信方法。

【請求項6】 前記スクランブルするステップは、前記バケットを送信する処理中に利用可能な空き時間を利用して前記元のデータの分割と前記バケットの組み立てを

行うことを特徴とする請求項1記載のスクランブル通信方法。

【請求項7】 前記復元するステップは、前記バケットを受信する処理中に利用可能な空き時間を利用して前記データ単位順序情報の復元と前記元のデータの再構成を行うことを特徴とする請求項1記載のスクランブル通信方法。

【請求項8】 前記スクランブルするステップは、所定の数の前記バケットをまとめて送信し、前記元のデータが該所定の数で割切れないときには、該スクランブルするステップは、少なくとも一つのパディングバケットを挿入してまとめて送信する該所定の数のバケットを形成することにより該バケットを組み立てることを特徴とする請求項1記載のスクランブル通信方法。

【請求項9】 受信側から送信側に、未受信のバケットの偽のバケット識別子を示す否定応答を送るステップと、

送信側から受信側に、該否定応答に示された偽のバケット識別子に基づいて、該未受信バケットに該当する偽の識別子を有するバケットを再送するステップと、
 20 を更に有することを特徴とする請求項1記載のスクランブル通信方法。

【請求項10】 ネットワークに設けられた中継装置において、該中継装置に設けられ、各バケット中に指定された宛先に対応する次の転送先または最終宛先を示す宛先変換テーブルに基づいて、各バケット中に指定された宛先を変更して、送信側から送信された前記バケットを中継するステップ、

を更に有することを特徴とする請求項1記載のスクランブル通信方法。

【請求項11】 ネットワークと、元のデータをバケットサイズの複数のデータ単位に分割し、該データ単位をバケットに格納して該バケットにスクランブルしたバケット順序を示す偽のバケット識別子を付与して該バケットを組み立てることにより該元のデータをスクランブルするスクランブル処理手段と、該バケットを該偽のバケット識別子に基づいてスクランブルしたバケット順序でネットワークに送信する送信手段と、を含む前記ネットワークに接続された送信装置と、

40 前記ネットワークから前記バケットを受信する受信手段と、前記偽のバケット識別子から真のデータ単位順序を示すデータ単位順序情報を復元し、該バケットに格納された前記データ単位から該データ単位順序情報に基づいて前記元のデータを再構成することにより、該バケットを復元する復元処理手段と、を含む前記ネットワークに接続された受信装置と、

を有することを特徴とするスクランブル通信システム。

【請求項12】 前記スクランブル処理手段は、スクランブルされていないバケット順序を示す真のバケット識別子を前記バケットに付与し、所定のスクランブルキー

に基づいて該真のバケット識別子を前記偽のバケット識別子に置き換えることにより該バケットを組み立て、前記復元処理手段は、前記所定のスクランブルキーに対応する所定のアセンブルキーに基づいて前記偽のバケット識別子を前記真のバケット識別子に変換し、前記元のデータを再構成するにあたって該真のバケット識別子を前記データ単位順序情報として用いることにより該データ単位順序を復元する、ことを特徴とする請求項11記載のスクランブル通信システム。

【請求項13】 前記スクランブル処理手段は、所定の計算手順に基づいて前記データ単位のメモリアドレスから前記偽のバケット識別子を直接計算して前記バケットを組み立て、前記復元処理手段は、前記所定の計算手順に基づいて前記偽のバケット識別子から前記データ単位のメモリアドレスを直接計算し、前記元のデータを再構成するにあたって該メモリアドレスを前記データ単位順序情報として用いることにより該データ単位順序情報を復元する、ことを特徴とする請求項11記載のスクランブル通信システム。

【請求項14】 前記スクランブル処理手段は、前記元のデータの分割と前記バケットの組み立てをプロトコル処理を実行することにより行うことを特徴とする請求項11記載のスクランブル通信システム。

【請求項15】 前記復元処理手段は、前記データ単位順序情報の復元と前記元のデータの再構成をプロトコル処理を実行することにより行うことを特徴とする請求項11記載のスクランブル通信システム。

【請求項16】 前記スクランブル処理手段は、前記送信手段による前記バケットを送信する処理中に利用可能な空き時間を利用して前記元のデータの分割と前記バケットの組み立てを行うことを特徴とする請求項11記載のスクランブル通信システム。

【請求項17】 前記復元処理手段は、前記受信手段による前記バケットを受信する処理中に利用可能な空き時間を利用して前記データ単位順序情報の復元と前記元のデータの再構成を行うことを特徴とする請求項11記載のスクランブル通信システム。

【請求項18】 前記送信手段は、所定の数の前記バケットをまとめて送信し、前記元のデータが所定の数で割切れないときには、前記スクランブル処理手段は、少なくとも一つのパディングバケットを挿入してまとめて送信する該所定の数のバケットを形成することにより該バケットを組み立てることを特徴とする請求項11記載のスクランブル通信システム。

【請求項19】 前記受信装置は、未受信バケットの偽のバケット識別子を示す否定応答を前記送信装置に送る手段を更に含む、前記送信装置は、該否定応答に示された偽のバケット識別子に基づいて、該未受信バケットに該当する偽の識別

子を有するバケットを再送する手段を更に含む、ことを特徴とする請求項11記載のスクランブル通信システム。

【請求項20】 各バケット中に指定された宛先に対応する次の転送先または最終宛先を示す宛先変換テーブルと、該宛先変換テーブルに基づいて各バケット中に指定された宛先を変更して、該変更された宛先を持つ各バケットを前記ネットワークに転送する転送手段とを含む前記ネットワークに設けられた中継装置、を更に有することを特徴とする請求項11記載のスクランブル通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、スクランブル通信方法及びシステムに係り、特に、情報の配布に対して課金するような有料情報の提供サービスにおいて、システム（ネットワーク）に非登録端末に対しては情報内容を取得することが困難（読みずらく）にし、登録者にとって配布情報の価値を高めるような情報配布サービスに適用するためのスクランブル通信方法及びシステムに関する。詳しくは、サーバ運用者にスクランブル処理時間の負担をかけることなく、また、端末利用者にもアセンブル（復号）処理の負担をかけることがなく、配布情報のスクランブル配送及び復号を実現するためのスクランブル通信方法及びシステムに関する。

【0002】

【従来の技術】サーバが端末に対してネットワークを介して情報を配布する時に、登録されていない端末に無断で受信され、利用されることを防ぐためには、送信するデータを分割し、かつ送信する順序を替えて（スクランブルをかけて）、受信後に利用者が事前に配布されている鍵で受信データを復元する方法がある。

【0003】図1は、従来のスクランブル配送のためのデータ転送方式を説明するための図である。同図に示すシステムは、サーバ1100、端末1200及びそれらを接続する通信ネットワーク1300より構成される。サーバ1100は、送信するデータのスクランブル処理を行うアプリケーション1110、スクランブル処理されたデータを送信するデータ送信部1120、通信制御部1130により構成される。端末1200は、受信したデータに復元処理を行うアプリケーション部1210、スクランブル処理されたデータを受信するデータ受信部1220、通信制御部1230より構成される。

【0004】同図に示すシステムでは、サーバ1100のアプリケーション部1110において送信前に送信すべき元のデータA全体にスクランブル処理を行い、データA'を生成し、データ送信部1120でデータA'を転送データ単位（バケット）に分割し、通信制御部1130及び通信ネットワーク1300を介して端末1200に送信する。端末1200は、転送データ単位（バケ

ット)を受け取り、データ受信部1220において、受信した転送データ単位(パケット)からデータA'を再構成する。

【0005】そして、アプリケーション部1210においてデータA'に復元処理を行い元のデータA全体を復元する。

【0006】尚、データ通信では、通常、サーバにおいて、送信データを分割して各転送データ単位(パケット)に識別番号を付与して転送し、データの送受信管理を行う。

【0007】

【発明が解決しようとする課題】しかしながら、上記の従来の方法では、送信装置において、例えば、データ転送前のファイル全体にスクランブルをかけるために、長時間を要する。また、同様に、受信装置において、受信したデータ全体を元の状態に復元するのにも長時間を要するため、利用者が受信したデータを取得するために時間がかかると共に煩わしいという問題がある。

【0008】ここで、図2および図3を参照して、従来のスクランブル配送を用いたデータ転送方式を更に詳しく説明する。

【0009】図2に示すように、従来のシステムでは、送信側はスクランブル処理(S1, S2, S3)を行うアプリケーション2100と送信処理(P1, P2)を行うプロトコル処理部2200を有し、受信側は受信処理(R1)を行うプロトコル処理部2400と復元処理(D1, D2)を行うアプリケーション2500とを有し、送信側と受信側は通信ネットワーク2300を介して接続される。

【0010】各部で行われる処理は、図3に示すように、以下の通りである。

【0011】(1)スクランブル処理

S1:データ全体を適当な分割サイズに分割する。

【0012】S2:シーケンス番号やメモリアドレス等のデータ識別番号(図3中で各分割データにつけられた数字)をS1で得た各分割データに付与する、または各分割データに割当てて別途管理する。

【0013】S3:分割データとそのデータ識別番号を所定のスクランブルキーに基づいて置き換える。

【0014】(2)送信処理

P1:送信するデータをパケットに格納する。ここで、パケットサイズは上記スクランブル処理(1)で用いた分割サイズとは異なる。

【0015】P2:順序を持ったパケット識別番号(シーケンス番号)pxを順序整合や再送等の送受信管理のためにパケットに付ける。

【0016】その後パケットは送信側から通信ネットワーク2300に送信され、受信側で受信される。一般に、受信パケットはネットワーク中で順序が入れ替わり、送信した通りの順序で受信側には届かない。

【0017】(3)受信処理

R1:受信パケットを所定のアセンブルキーに基づいて正しいアドレスに格納して、データ全体を再構成する。

【0018】(4)復元処理

D1:パケットに格納された分割データの元のデータ識別番号を所定のアセンブルキーに基づいて復元する。

【0019】D2:復元された元のデータ識別番号に基づいて分割データの順序を入れ替えて元のデータを復元する。

10 【0020】尚、送信処理P1, P2と受信処理R1のプロトコル処理はスクランブル配送をするかしないかに拘らずパケットによるデータ通信では必須の処理である。

【0021】この図3に示す従来の方式では、送信処理とは別にスクランブル処理を行い、受信処理とは別に復元処理を行っている。このため、従来のスクランブル配送を用いたデータ転送方式では、スクランブル処理、復元処理の全体が追加の処理量と処理時間を必要とするものであった。

20 【0022】また、従来はネットワーク加入者の設備(サーバ、端末)と接続している回線設備と中継を行うネットワーク設備が単一の通信事業者内で閉じられたネットワークで運用されているが、近年、ネットワークのインタフェースが多数の通信事業者やVAN業者(付加価値通信業者)にも開示され、複数事業者により設備間が結合された複合的なネットワークが提供されつつある。従来の単一業者内のネットワークでは、加入者回線、中継設備等の物理的なネットワーク自体が外部からのアクセスが難しく、また、設備間のインタフェースも公開されていなかったため、通信データの機密性が守られている。しかし、複数業者によるサービスの場合は、各業者設備間の接続点、あるいは、各業者の中継設備と端末接続している回線との接続点において、非登録利用者から無断で通信データが取得される可能性がでてきている。

30 【0023】本発明は、上記課題に鑑みてなされたもので、送信側や受信側におけるスクランブル処理や復元処理に必要な処理量や処理時間を軽減することが可能なスクランブル通信方法およびシステムを提供することを目的とする。

40 【0024】また、本発明は、複数のネットワークが接続された複合的なネットワークを用いる場合に信頼性の高い情報通信サービスを実現することが可能なスクランブル通信方法およびシステムを提供することを目的とする。

【0025】

【課題を解決するための手段】本発明は、ネットワークで接続された送信側と受信側間のスクランブル通信方法であって、送信側において、元のデータをパケットサイズの複数のデータ単位に分割し、該データ単位をパケッ

トに格納して該バケットにスクランブルしたバケット順序を示す偽のバケット識別子を付与して該バケットを組み立て、該バケットを該偽のバケット識別子に基づいてスクランブルしたバケット順序でネットワークに送信することにより、該元のデータをスクランブルするステップと、受信側において、前記偽のバケット識別子から真のデータ単位順序を示すデータ単位順序情報を復元し、前記バケットに格納された前記データ単位から該データ単位順序情報に基づいて前記元のデータを再構成することにより、ネットワークから受信した前記バケットを復元するステップと、を有することを特徴とするスクランブル通信方法を提供する。

【0026】さらに、本発明では、前記スクランブルするステップは、スクランブルされていないバケット順序を示す真のバケット識別子を前記バケットに付与し、所定のスクランブルキーに基づいて該真のバケット識別子を前記偽のバケット識別子に置き換えることにより該バケットを組み立て、前記復元するステップは、前記所定のスクランブルキーに対応する所定のアセンブリキーに基づいて前記偽のバケット識別子を前記真のバケット識別子に変換し、前記元のデータを再構成するにあたって該真のバケット識別子を前記データ単位順序情報として用いることにより該データ単位順序情報を復元する、ことを特徴とする。

【0027】さらに、本発明では、前記スクランブルするステップは、所定の計算手順に基づいて前記データ単位のメモリアドレスから前記偽のバケット識別子を直接計算して前記バケットを組み立て、前記復元するステップは、前記所定の計算手順に基づいて前記の偽バケット識別子から前記データ単位のメモリアドレスを直接計算し、前記元のデータを再構成するにあたって該メモリアドレスを前記データ単位順序情報として用いることにより該データ単位順序情報を復元する、ことを特徴とする。

【0028】さらに、本発明では、前記スクランブルするステップは、送信側におけるプロトコル処理により行われることを特徴とする。

【0029】さらに、本発明では、前記復元するステップは、受信側におけるプロトコル処理により行われることを特徴とする。

【0030】さらに、本発明では、前記スクランブルするステップは、前記バケットを送信する処理中に利用可能な空き時間を利用して前記元のデータの分割と前記バケットの組み立てを行うことを特徴とする。

【0031】さらに、本発明では、前記復元するステップは、前記バケットを受信する処理中に利用可能な空き時間を利用して前記データ単位順序情報の復元と前記元のデータの再構成を行うことを特徴とする。

【0032】さらに、本発明では、前記スクランブルするステップは、所定の数の前記バケットをまとめて送信

し、前記元のデータが該所定の数で割切れないときには、該スクランブルするステップは、少なくとも一つのパディングバケットを挿入してまとめて送信する該所定の数のバケットを形成することにより該バケットを組み立てることを特徴とする。

【0033】さらに、本発明では、受信側から送信側に、未受信のバケットの偽のバケット識別子を示す否定応答を送るステップと、送信側から受信側に、該否定応答に示された偽のバケット識別子に基づいて、該未受信バケットに該当する偽の識別子を有するバケットを再送するステップと、を更に有することを特徴とする。

【0034】さらに、本発明では、ネットワークに設けられた中継装置において、該中継装置に設けられ、各バケット中に指定された宛先に対応する次の転送先または最終宛先を示す宛先変換テーブルに基づいて、各バケット中に指定された宛先を変更して、送信側から送信された前記バケットを中継するステップ、を更に有することを特徴とする。

【0035】また、本発明は、ネットワークと、元のデータをバケットサイズの複数のデータ単位に分割し、該データ単位をバケットに格納して該バケットにスクランブルしたバケット順序を示す偽のバケット識別子を付与して該バケットを組み立てることにより該元のデータをスクランブルするスクランブル処理手段と、該バケットを該偽のバケット識別子に基づいてスクランブルしたバケット順序でネットワークに送信する送信手段と、を含む前記ネットワークに接続された送信装置と、前記ネットワークから前記バケットを受信する受信手段と、前記偽のバケット識別子から真のデータ単位順序を示すデータ単位順序情報を復元し、該バケットに格納された前記データ単位から該データ単位順序情報に基づいて前記元のデータを再構成することにより、該バケットを復元する復元処理手段と、を含む前記ネットワークに接続された受信装置と、を有することを特徴とするスクランブル通信システムを提供する。

【0036】さらに、本発明では、前記スクランブル処理手段は、スクランブルされていないバケット順序を示す真のバケット識別子を前記バケットに付与し、所定のスクランブルキーに基づいて該真のバケット識別子を前記偽のバケット識別子に置き換えることにより該バケットを組み立て、前記復元処理手段は、前記所定のスクランブルキーに対応する所定のアセンブリキーに基づいて前記偽のバケット識別子を前記真のバケット識別子に変換し、前記元のデータを再構成するにあたって該真のバケット識別子を前記データ単位順序情報として用いることにより該データ単位順序情報を復元する、ことを特徴とする。

【0037】さらに、本発明では、前記スクランブル処理手段は、所定の計算手順に基づいて前記データ単位のメモリアドレスから前記偽のバケット識別子を直接計算

して前記バケットを組み立て、前記復元処理手段は、前記所定の計算手順に基づいて前記偽のバケット識別子から前記データ単位のメモリアドレスを直接計算し、前記元のデータを再構成するにあたって該メモリアドレスを前記データ単位順序情報として用いることにより該データ単位順序情報を復元する、ことを特徴とする。

【0038】さらに、本発明では、前記スクランブル処理手段は、前記元のデータの分割と前記バケットの組み立てをプロトコル処理を実行することにより行うことを特徴とする。

【0039】さらに、本発明では、前記復元処理手段は、前記データ単位順序情報の復元と前記元のデータの再構成をプロトコル処理を実行することにより行うことを特徴とする。

【0040】さらに、本発明では、前記スクランブル処理手段は、前記送信手段による前記バケットを送信する処理中に利用可能な空き時間を利用して前記元のデータの分割と前記バケットの組み立てを行うことを特徴とする。

【0041】さらに、本発明では、前記復元処理手段は、前記受信手段による前記バケットを受信する処理中に利用可能な空き時間を利用して前記データ単位順序情報の復元と前記元のデータの再構成を行うことを特徴とする。

【0042】さらに、本発明では、前記送信手段は、所定の数の前記バケットをまとめて送信し、前記元のデータが該所定の数で割切れないときには、前記スクランブル処理手段は、少なくとも一つのパディングバケットを挿入してまとめて送信する該所定の数のバケットを形成することにより該バケットを組み立てることを特徴とする。

【0043】さらに、本発明では、前記受信装置は、未受信バケットの偽のバケット識別子を示す否定応答を前記送信装置に送る手段を更に含み、前記送信装置は、該否定応答に示された偽のバケット識別子に基づいて、該未受信バケットに該当する偽の識別子を有するバケットを再送する手段を更に含む、ことを特徴とする。

【0044】さらに、本発明では、各バケット中に指定された宛先に対応する次の転送先または最終宛先を示す宛先変換テーブルと、該宛先変換テーブルに基づいて各バケット中に指定された宛先を変更して、該変更された宛先を持つ各バケットを前記ネットワークに転送する転送手段とを含む前記ネットワークに設けられた中継装置、を更に有することを特徴とする。

【0045】

【発明の実施の形態】まず、図4から図7を参照して、本発明のスクランブル通信方法およびシステムの主要な特徴について説明する。

【0046】図4は本発明のスクランブル通信システムの基本構成を示しており、このシステムでは、送信側は

データを提供するアプリケーション10とスクランブル処理(S3)と送信処理(P1(S1)、P2(S2))を行うプロトコル処理部20を有し、受信側は受信処理(R1(D2))と復元処理(D1)を行うプロトコル処理部40とデータを取得するアプリケーション50とを有し、送信側と受信側は通信ネットワーク30を介して接続される。

【0047】各部で行われる処理は、図5に示すように、以下の通りである。

10 【0048】(a) スクランブルしながらバケット送信処理

P1(S1)：データ全体をスクランブルに適当な分割サイズに等しいバケットサイズに分割する。図5中で各分割データにつけられた数字は各分割データを識別するための分割データのシーケンス番号である。

【0049】P2(S2)：バケットを組み立てる。

【0050】S3：偽のバケット識別番号pfxを各バケットに付与する。

20 【0051】その後バケットは送信側から通信ネットワーク30に送信され、受信側で受信される。一般に、受信バケットはネットワーク中で順序が入れ替わり、送信した通りの順序で受信側には届かない。

【0052】(b) 復元しながらバケット受信処理
D1：各バケットの真のバケット識別番号pxを復元しながら、バケットを受信する。

【0053】R1(D2)：バケットから元のデータを再構成する。

30 【0054】この本発明のスクランブル通信方法では、スクランブル処理S1、S2は送信処理P1、P2の一部として行い、復元処理D2は受信処理R1の一部として行われる。従って、スクランブル配送を行う場合でも、S1、S2およびD2の処理はプロトコル処理により行われるので、これらの処理に追加の処理量や処理時間を必要としない。このため、本発明では、スクランブル処理と復元処理をプロトコル処理の一部として実行することによりスクランブル処理と復元処理の大半(S1、S2、D2)にかかる処理量と処理時間を削減することが可能となる。

40 【0055】より詳細には、以下に詳述する本発明のスクランブル通信の第1の実施形態では、スクランブル通信は図6に示すように、以下の通り行われる。

【0056】即ち、スクランブルしながらのバケット送信処理では、P1(S1)で、データ全体をスクランブルに適当な分割サイズに等しいバケットサイズに分割する。

【0057】そして、P2(S2)で、各バケットに真のバケット識別番号pxを付与しながらバケットを組み立てる。

50 【0058】そして、S3で、真のバケット識別番号pxを偽のバケット識別番号pfxで置き換える。

【0059】一方、復元しながらのバケット受信処理では、D1で、偽のバケット識別番号pfxを真のバケット識別番号pxに変換しながらバケットを受信する。

【0060】そして、R1(D2)で、真のバケット識別番号に基づいてバケットから元のデータ全体を再構成する。

【0061】これに対して、以下に詳述する本発明のスクランブル通信の第2の実施形態では、スクランブル通信は図7に示すように、以下の通り行われる。

【0062】即ち、スクランブルしながらのバケット送信処理では、P1(S1)で、データ全体をスクランブルに
10 適当な分割サイズに等しいバケットサイズに分割する。

【0063】そして、P2(S2)とS3で、偽のバケット識別番号pfxを各バケット中の分割データのメモリアドレスから直接計算して各バケットに付与しながらバケットを組み立てる。

【0064】一方、復元しながらのバケット受信処理では、D1で、偽のバケット識別番号pfxから分割データのメモリアドレスを直接計算しながらバケットを受信
20 する。

【0065】そして、R1(D2)で、分割データのメモリアドレスに基づいてバケットから元のデータ全体を再構成する。

【0066】次に、図8から図14を参照して、本発明のスクランブル通信方法およびシステムの第1の実施形態について詳細に説明する。

【0067】図8は、本発明の第1の実施形態を適用する情報配送システムの構成を示す。同図に示すシステムは、サーバ100、複数の端末200-1、200-2、200-nとこれらを接続するネットワーク300より構成される。サーバ100は、ネットワーク300を介して、複数の端末200-1、200-2、200-nに対して、スクランブル処理されたデータを送信し、端末200において、それぞれ受信したデータを復号する。

【0068】図9は、第1の実施形態のデータ転送におけるスクランブル配送を説明するための図である。サーバ100は、アプリケーション部110、データ送信部120、通信制御部130より構成される。

【0069】アプリケーション部110は、端末200に送信すべきデータ全体をデータ送信部120に渡す。

【0070】データ送信部120は、データ全体をバケットに分割し、所定のスクランブルキーに基づいて、シーケンス番号(識別番号)を入れ替えて、通信制御部130に転送する。

【0071】図10は、図9のサーバ100におけるデータ送信部120の構成を示す。データ送信部120は、例えば1ファイル分のデータをアプリケーション部110から渡されると、当該ファイルのデータをバケッ
50

トに分割する処理を行う。データ送信部120は、バケット分割部121、スクランブルキー格納部122、及びスクランブル処理部123及び空き時間監視部124より構成される。バケット分割部121は、アプリケーション部110から渡された全データをバケット単位に分割して、スクランブル処理部123に転送する。スクランブルキー格納部122は、端末200と共有するスクランブルキーを保持する。スクランブル処理部123は、スクランブルキー格納部122を参照して、バケット分割部121で分割されたバケット単位にスクランブルキーに基づいてバケットシーケンス番号を付与して、図11に示すようなフォーマットのデータバケットを生成する。

【0072】図11に示すデータバケット400は、宛先401、バケットシーケンス番号402及びユーザデータ部403より構成され、宛先401には、受信装置の宛先アドレスを設定し、バケットシーケンス番号402には、スクランブル処理部123で取得したバケットシーケンス番号を設定し、ユーザデータ部403には、分割された1単位分のデータ(メッセージ)を設定する。なお、宛先401が付与されない場合には、データは、通信階層上、下階層のバケットに格納される。

【0073】なお、空き時間監視部124については、後述する。

【0074】サーバ100の通信制御部130は、データ送信部120で生成されたデータバケット400をネットワーク300を介して端末200に送信する。

【0075】端末200は、アプリケーション部210、データ受信部220及び通信制御部230より構成される。

【0076】通信制御部230は、サーバ100から転送されたデータバケット400を受信して、当該バケットをデータ受信部220に転送する。

【0077】データ受信部220は、所定のアセンブル(復号)キーによりデータバケット400のバケットシーケンス番号402を復号しながら、データ全体を再構成し、アプリケーション部210に転送する。

【0078】図12は、図9の端末200におけるデータ受信部220の構成を示す。データ受信部220は、復号部221、アセンブルキー格納部222、データ結合部223及び空き時間監視部224より構成される。

【0079】アセンブルキー格納部222は、サーバ100と共有するデータバケット400のバケットシーケンス番号402を復号するためのアセンブルキーを格納している。復号部221は、通信制御部230より渡されたデータバケット400に対しアセンブルキー格納部222のアセンブルキーを参照して、バケットシーケンス番号402を復号する。

【0080】データ結合部223は、復号部221で復号された、データバケットを保持しておき、全てのデー

タバケット400を受け取った時点で、シーケンス番号に基づいてバケットを正規のデータの順に並べ替えて元のデータ（サーバ側のデータ）を再構成する。

【0081】なお、空き時間監視部224については、後述する。

【0082】この第1の実施形態では、上記の送信前と受信後の処理をサーバ100の送信処理の空き時間及び端末200の受信処理の空き時間に行う。空き時間は、サーバ100及び端末200の空き時間監視部124、224がそれぞれの通信制御部130、230を監視して送信処理または受信処理を行っていない時間（空き時間）を検出する。空き時間が検出されると、サーバ100の空き時間監視部124は、バケット分割部121を起動し、また、端末200の空き時間監視部224は、復号部221を起動する。

【0083】図13は、第1の実施形態におけるサーバ側のデータ送信の空き時間を示し、図14は、第1の実施形態における端末側のデータ受信の空き時間を示す。図13は、サーバ100側において、バケットをn個連続転送し、一定時間待つという送信速度調整を行っている場合の送信空き時間を例示している。図14は、端末200側において、各バケットの受信処理の間の空き時間、及び未受信のバケットがあるため、次のバケットを待っている間にタイムアウトした場合のタイムアウトまでの空き時間を例示している。後者の場合、端末200では、タイムアウト後にサーバ100への応答生成処理を行っている。したがって、サーバ100のデータ送信部120は、図13において、送信空き時間a、b、cの間で、上記の送信前の処理を行って、端末200に送信するデータバケット400を生成する。また、端末200のデータ受信部220は、図14において、受信空き時間x、y、zの間で上記の受信後の処理を行って、サーバ100から受け取ったデータバケットの復号処理を行う。

【0084】ここで、以下の説明で用いる用語をいくつか定義しておく。

【0085】以下の説明において、サーバ100のアプリケーション部110から送信を指示されたデータ全体をメッセージと呼ぶ。また、メッセージを分割して転送するデータの単位をデータバケットと呼ぶ。

【0086】データバケットは、前述の図11に示す構成であり、メッセージを分割した情報をユーザデータ部403に格納し、メッセージの先頭から対応付けてバケットシーケンス番号402を1から順に付与する。データバケットには宛先401を付与して端末200に配送する。宛先401を付けない場合には、データは、通信階層上、下位層のバケットに格納されて端末に配布される。

【0087】データバケットの長さは、必要とするスクランブルの粒度（細かさ）に応じて設定する。長さを短

くすればするほど、情報がより解読しにくくなる。以下では、64バケット単位のブロック内のスクランブル転送の例を示すが、このブロックを構成するバケット数を大きくすることにより、情報がより解読しにくくなる。

【0088】「スクランブルキーは、サーバ100が所有し、復元のためのアセンブルキーは、サーバ100が各端末毎に、ファイル転送等の通信によって、または、情報配送サービスに登録されている端末にオフラインによって事前に配布しておく。」

10 【0089】スクランブル転送が行われていることや、使用したバディグの値についてはサーバ100から端末200にコネクション確立要求バケット等の手段で、データ転送前に通知されていることとする。

【0090】次に、上記の定義に基づいてサーバ100の送信手順について説明する。

【0091】転送時に速度調節等によりデータバケット転送の空き時間を利用して以下の操作を行うものとする。

20 【0092】(1) 64バケット単位のスクランブル64バケットの中で、バケットシーケンス番号を入れ替えて、偽のバケットシーケンス番号を付与する。そして、偽のバケットシーケンス番号の順にデータバケットを転送する処理を64バケット分繰り返す。

【0093】(2) バディグ

サーバ100のアプリケーション部110から与えられたメッセージが64で割り切れない場合には、バディグバケット（空きバケット）を挿入して、得られる疑似メッセージを64の倍数とする。

30 【0094】一方、端末200におけるデータバケットの復号処理は、データ受信部220がデータバケットを受信する毎に、受信処理の空き時間にアセンブルキーに基づいてバケットシーケンス番号402を真の値に置き換える。

【0095】次に、第1の実施形態に基づいて、スクランブルキー及びアセンブルキーを使用して、スクランブル配送及び復号を行う具体的な例を説明する。

【0096】(1) サーバ100から端末200へのスクランブル配送：この例では、簡単のために8バケットに基づく説明とする。

40 【0097】サーバ100において、メッセージバケットのシーケンス番号列を“1, 2, 3, 4, 5, 6, 7, 8”とし、スクランブルキー格納部122に格納されているスクランブルキーを、“6, 3, 7, 2, 1, 8, 4, 5”とする。このスクランブルキーは、5番目に位置する“1”によってバケットシーケンス番号“5”のバケットを1番目に送信し、4番目に位置する“2”によってバケットシーケンス番号“4”のバケットを2番目に送信し、…ということを表している。

【0098】これにより、ネットワーク300上では、偽のバケットシーケンス番号列は、“1, 2, 3, 4,

☆

5, 6, 7, 8”であるが、真のバケットシーケンス番号列は、“5, 4, 2, 7, 8, 1, 3, 6”である。

【0099】上記の例は、8バケットを用いた例であるが、64バケットを用いる場合も同様の手順で行う。

【0100】サーバ100は、空き時間において、このスクランブル配送を繰り返す。最初は、バケットシーケンス番号“1～64”番に対して上記の処理を行い、次に、“65～128”番に対して行う。スクランブルキーは同じで、バケット番号のモジュロ64（64で割った余り、0は64として扱う）に対してスクランブルをかける。この処理を64バケット単位に全てのデータに対して行う。

【0101】（2）端末200における復号
受信側の端末200が上記のバケットシーケンス番号列、“1, 2, 3, 4, 5, 6, 7, 8”のバケットを受信すると、端末200のアセムルキー格納部222で保持するアセムルキーは、“5, 4, 2, 7, 8, 1, 3, 6”であり、これは真のバケットシーケンス番号列と同じである。このアセムルキーは、スクランブルキーより容易に生成可能である。このアセムルキーは、1番目に位置する“5”によって偽のバケットシーケンス番号“1”を真のバケットシーケンス番号“5”に置き換えて受信し、2番目に位置する“4”によって偽のバケットシーケンス番号“2”を真のバケットシーケンス番号“4”に置き換えて受信し…ということを表している。この復号処理を受信した全てのバケットについて行う。

【0102】（3）再送のための応答：サーバ100が端末200の未受信バケットに対して再送を行う処理を説明する。

【0103】端末200は、サーバ100に対する応答に未受信バケットの偽のバケットシーケンス番号を入れてサーバ100に送出する（否定応答）。これにより、サーバ100は、再送バケットについても最初のデータ転送と同じスクランブル処理されているものを再送する。

【0104】（4）受信後の処理
端末200のデータ結合部223は、メッセージ全体を受信後、パディングバケットを取り除き、真のバケットシーケンス番号に従って正規の順に並び替えを行い、元のメッセージを得る。

【0105】尚、上述した第1の実施形態では、サーバ100、端末200の双方に本発明を適用した例を示したが、上記の端末200のバケット受信以降の処理を直に行なわずに、単に利用者に配布情報を渡して、その後利用者が別アプリケーション等でアセムルキーを利用して情報を復元し、最後にメッセージが所定のバケット数で割り切れない場合に用いるパディングバケットを取り除いて、元の情報を得るようにすることも可能である。これは、同一の端末を登録利用者も非登録利用者も

使用するような場合に有効である。

【0106】これにより、復号処理に関する負担は利用者にかかるものの、非登録利用者による配布情報の利用を防ぎ、登録利用者に対してのみ有料情報の配布が可能となる。

【0107】次に図15と図16を参照して、本発明のスクランブル通信方法およびシステムの第2の実施形態について詳細に説明する。

【0108】この第2の実施形態においては、情報配送システムの構成は図8に示すものと同じであり、サーバ100と端末200の構成も図9に示すものと同じである。

【0109】図15は、第2の実施形態におけるサーバ100のデータ送信部120の構成を示す。同図に示すデータ送信部120は、バケット組み立て部125とスクランブルキー格納部122より構成される。データ送信部120のバケット組み立て部125は、サーバ100のアプリケーション部110のメモリ上からデータ単位を取り出して、宛先、偽のバケットシーケンス番号を付与してデータバケットを生成する。これにより、予め生成したデータバケットに対してバケットシーケンス番号の変換処理を行う第1の実施形態の場合に比べて、変換処理が不要となる分だけ処理負荷、処理時間が少なくて済む。

【0110】即ち、バケットシーケンス番号を付けてデータバケットを生成するという通信のために必要な手順（処理）に、偽のバケットシーケンス番号を付けるというスクランブルの手順（処理）が一体的に含まれるので、この分の処理が少なくて済むことになる。

【0111】図16は、第2の実施形態における端末200のデータ受信部220の構成を示す。同図に示すデータ受信部220は、バケット分割部225とアセムルキー格納部222より構成される。データ受信部220において、復号を行う際に、受信したデータ単位の偽バケットシーケンス番号から真のデータ格納位置（メモリアドレス）を算出して、データ受信を行うので、一旦受信データを蓄積してからデータ単位を真のデータ格納位置に並べ替える従来の場合に比べて、データ単位並べ替え処理が不要となる分だけ処理負荷、処理時間が少なくて済む。

【0112】即ち、受信データバケットのバケットシーケンス番号によりデータを格納するという通信のために必要な手順（処理）に真のデータ格納位置を復元するというアセムルの手順（処理）が一体的に含まれるため、この分の処理が少なくて済むことになる。

【0113】ここで、サーバ100におけるデータ単位のメモリアドレスから偽のバケットシーケンス番号を求める計算と、端末200における偽のバケットシーケンス番号からデータ単位の真のメモリアドレスを求める計算には、以下のような処理負荷の殆どない単純な計算を

用いることができる。ここでも、簡単のために前述同様8バケットに基づく説明とする。

【0114】即ち、サーバ100のスクランブルキー格納部122に格納されているスクランブルキーに対応する、端末200のアセンブルキー格納部222に格納されている真のバケットシーケンス番号列（アセンブルキ

偽のバケットシーケンス番号

pf1

pf2

pf3

pf4

pf5

pf6

pf7

pf8

同様に、偽のバケットシーケンス番号pf9からpf16に対して、対応するメモリアドレスは次のように求め※

偽のバケットシーケンス番号

pf9

pf10

pf11

pf12

pf13

pf14

pf15

pf16

一般には、偽のバケットシーケンス番号pf(8n+1)からpf(8n+8)に対応するメモリアドレスは、次のように表される。但し、nは0以上の整数とす★

偽のバケットシーケンス番号

pf(8n+1)

pf(8n+2)

pf(8n+3)

pf(8n+4)

pf(8n+5)

pf(8n+6)

pf(8n+7)

pf(8n+8)

端末200のデータ受信部220では、サーバ100と同じ計算手順を共有することにより、上述した端末200のアセンブルキー格納部222に格納されている真のバケットシーケンス番号列（アセンブルキー）に基づいて、データ単位の真のメモリアドレスを上記の対応に従って偽のバケットシーケンス番号から求めることができる。これにより、データ単位はサーバ100と端末200で同一のメモリアドレスを持つことが可能となる。

【0118】但し、前述した端末200でバケット受信以降の処理を行わずに、単に利用者に配布情報を渡し、その後、利用者側でアセンブルキーを利用して情報を復元し、パディングバケットを除去して元の情報に復

※一) “5, 4, 2, 7, 8, 1, 3, 6”に基づいて、サーバ100のデータ送信部120では、偽のバケットシーケンス番号pf1からpf8で送信されるデータ単位のメモリアドレスは、先頭メモリアドレスIとデータ単位サイズdを用いて、次のように順に求められる。

【0115】

メモリアドレス

$I + (5 - 1) d$

$I + (4 - 1) d$

$I + (2 - 1) d$

$I + (7 - 1) d$

$I + (8 - 1) d$

$I + (1 - 1) d$

$I + (3 - 1) d$

$I + (6 - 1) d$

※られる。

【0116】

メモリアドレス

$I + (8 + 4) d$

$I + (8 + 3) d$

$I + (8 + 1) d$

$I + (8 + 6) d$

$I + (8 + 7) d$

$I + (8 + 0) d$

$I + (8 + 2) d$

$I + (8 + 5) d$

★る。

【0117】

メモリアドレス

$I + (8n + 4) d$

$I + (8n + 3) d$

$I + (8n + 1) d$

$I + (8n + 6) d$

$I + (8n + 7) d$

$I + (8n + 0) d$

$I + (8n + 2) d$

$I + (8n + 5) d$

元するような場合には、上記のようなデータ格納方法を用いない。

【0119】上記のように、第2の実施形態では、サーバ100のバケット組み立て部125において、端末200と共通に与えられている計算手順を用いることにより、データ単位のメモリアドレスから直接偽のバケットシーケンス番号を取得して、これをデータバケットに付与し、また、端末200のバケット分割部225において、サーバ100と共通に与えられている計算手順を用いることにより、偽のバケットシーケンス番号から直接データ単位の真のデータ格納位置を取得して、当該位置にデータを格納する。

【0120】次に、図17から図19を参照して、本発明のスクランブル通信方法およびシステムの第3の実施形態について詳細に説明する。

【0121】上記の第1及び第2の実施形態では、サーバ/端末のエンドエンド間のスクランブル通信の例を示したが、本発明のスクランブル通信は「サーバ/端末」のみならず、「サーバ/中継装置」、「中継装置/中継装置」、「中継装置/端末」等、各装置間の通信に個別に必要に応じて適用できる。

【0122】図17は、本発明の第3の実施形態を適用する中継装置を含む情報配送システムの構成を示す。

【0123】同図は、上記の図8のサーバと端末のエンド/エンド間でスクランブル通信を行う構成に加えて、サーバ100がネットワーク300内の中継装置300-1に回線で接続され、中継装置300-7から300-n間が回線で接続され、中継装置300-2と端末200-1、端末200-2が接続されている。図17に示すシステムでは、サーバ/中継装置、中継装置間、中継装置/端末間の各箇所において必要に応じて個別にスクランブル通信を行う。

【0124】このようにネットワーク300内の中継装置を介してスクランブル通信を行うことにより、複合化されたネットワークにおける通信においても秘匿性を保持した通信が可能となる。

【0125】なお、図17において、ネットワーク及びサーバ/中継装置間の回線及び中継装置間の回線及び中継装置/端末間の回線には地上のISDN、専用線等の有線、衛星、セルラ等の無線の各種伝送形態を利用可能である。また、中継装置は、パケット交換機、ATM交換機、ルータ等が利用できる。

【0126】図18は、第3の実施形態の中継装置300-nの構成を示す。同図に示す中継装置300-nは、転送処理部310、中継受信部320及び中継送信部330より構成され、中継送信部320は、データ送信部321と通信制御部322より構成され、中継送信部330は、データ送信部331と通信制御部332より構成され、データ受信部321及び通信制御部322は、図9に示す端末200のデータ受信部220及び通信制御部230と同様の機能を有する。転送処理部310は、中継するデータパケットの宛先交換処理を行う。

【0127】図19は、図18の中継装置300-nにおける転送処理部310の構成を示す。同図に示す転送処理部310は、宛先交換テーブルを格納する宛先交換テーブル格納部311、受信したデータパケットを蓄積する転送データバッファ312及び、宛先変更処理を実行する転送データ制御部313を有する。このような中継装置は、蓄積交換型の中継装置で通常用いられるものである。

【0128】このような構成を有する第3の実施形態の中継装置300-nによるデータパケット中継の手順

は、次の通りである。

【0129】転送処理部310において、データ受信部321からデータパケットを受け取ると、宛先交換テーブル格納部311の宛先交換テーブルを参照して、データパケットの宛先を転送先の中継装置あるいは、最終の配送先の端末200の宛先に変換する。データ単位が適当数溜ったところで、データ送信部331に送信要求する。データ転送部331では、相手の中継装置あるいは端末200との間でパケットの転送を行う。

【0130】以上の手順における転送処理部310の動作は、次の通りである。転送データ制御部313は、受信データを転送データバッファ312に蓄積し、宛先交換テーブル格納部311の宛先交換テーブルを参照してデータパケットの宛先を変更してデータパケットを転送する。

【0131】次に、図20を参照して、情報配送サービス加入者と情報サービスセンタとの間に本発明のスクランブル通信を適用した電子新聞配送システムの例を説明する。

【0132】図20は、本発明を適用した電子新聞配送システムの一例を示す。

【0133】同図に示すシステムは、サーバ100を有する配送センタ500、通信ネットワーク300、複数の端末200、端末200を有する販売所600より構成される。

【0134】端末200を持たない購読者には、販売所600で複製された電子新聞が販売所600より配布される。

【0135】サーバ100から端末200にマルチキャスト通信により、毎朝、一斉に電子新聞を配布する。その際、本発明のスクランブル通信方法に従って情報のスクランブルを行う。購読を登録している利用者の端末200には予め安全な方法で復元鍵（アセンブルキーを表す数字列）を配布しておく。非登録利用者は、通信を傍受することはできても復元鍵がないので、容易に解読することはできない。

【0136】例えば、同図において、端末Aの利用者は復元鍵240を有しているため、当該通信による購読が可能であるが、端末Bの非登録利用者は復元鍵を有していないため、購読が不可能である。

【0137】なお、復元鍵を定期的に変更し、購読料が未払いの利用者には最新の復元鍵を配布しないようにすることにより、そのような利用者は電子新聞を受信できても解読が困難となるようにすることが可能である。

【0138】次に、図21を参照して、本発明のスクランブル通信の情報ネットワークへの部分的な適用を説明する。

【0139】図21は、本発明を部分的に適用した情報ネットワークシステムの一例を示す。同図において、楕円で示される700aから700fは情報ネットワーク

である。ネットワーク700aは、企業本店内の中継装置または、端末装置Aを有し、ネットワーク700fは企業支店内の中継装置または端末装置Dを有する。ネットワーク700cは中継装置Bと中継装置Cを有する。

【0140】このような情報ネットワークシステムにおいて、ネットワーク700aの企業本店内の端末Aとネットワーク700fの端末D間において通信を行う場合に、長距離ネットワーク700cの中継装置と企業の端末A、Dとの間に本発明を適用する。このとき、利用者企業と長距離ネットワーク700cとの間に公開接続点や安全が保証されない地域ネットワーク700bを組む場合に、以下のようにして通信を行うことが考えられる。

【0141】(1) 企業本店の端末Aと長距離ネットワーク700cの中継装置Bとの間で本発明を適用してスクランブル通信を行うことが可能である。

【0142】(2) 長距離ネットワーク700cは多数の接続点を公開しており、不正アクセスの可能性があるので、長距離ネットワーク700cの中継装置B-C間に本発明を適用してスクランブル通信を行うことが可能である。

【0143】(3) 長距離ネットワーク700cと地域ネットワーク700eの中継装置E-C間に本発明を適用してスクランブル通信を行うことが可能である。

【0144】このように、あるネットワーク毎に順次本発明によるスクランブル通信を適用していくことにより、秘匿性を保証することが可能となる。

【0145】以上の説明では、A、Dを企業内の端末として説明したが、A、Dを企業内の中継装置とし、A、Dを企業内の複数の端末に接続して通信を行う場合にも本発明を同様に適用できる。

【0146】なお、本発明は、上記の実施形態に限定されことなく、特許請求の範囲内で種々変更・応用が可能である。

【0147】

【発明の効果】以上説明したように、本発明のスクランブル通信方法およびシステムによれば、スクランブル処理と復元処理をプロトコル処理の一部として実行することによりスクランブル処理と復元処理の大半にかかる処理量と処理時間を削減することが可能となるので、送信側や受信側におけるスクランブル処理や復元処理に必要な処理量や処理時間を軽減することが可能となる。

【0148】また、本発明のスクランブル通信方法およびシステムによれば、ネットワーク中の適当な箇所に個別にスクランブル通信を適用して中継装置を介在させた通信を行うことにより、複数のネットワークが接続された複合的なネットワークを用いる場合に信頼性の高い情報通信サービスを実現することが可能となる。

【図面の簡単な説明】

【図1】従来のスクランブル通信システムを示すブロッ

10

20

30

40

50

ク図。

【図2】従来のスクランブル通信システムの機能構成を示すブロック図。

【図3】従来のスクランブル通信方法の処理の流れを示す図。

【図4】本発明のスクランブル通信システムの機能構成を示すブロック図。

【図5】本発明のスクランブル通信方法の処理の流れを示す図。

【図6】本発明のスクランブル通信方法の第1の実施形態における処理の流れを示す図。

【図7】本発明のスクランブル通信方法の第2の実施形態における処理の流れを示す図。

【図8】本発明の第1、第2の実施形態における情報配送システムを示すブロック図。

【図9】本発明の第1、第2の実施形態におけるスクランブル通信システムを示すブロック図。

【図10】本発明の第1の実施形態における図9のスクランブル通信システムのデータ送信部を示すブロック図。

【図11】本発明で用いるデータパケットのフォーマットを示す図。

【図12】本発明の第1の実施形態における図9のスクランブル通信システムのデータ受信部を示すブロック図。

【図13】本発明の第1の実施形態において用いる送信側の空き時間を示す図。

【図14】本発明の第1の実施形態において用いる受信側の空き時間を示す図。

【図15】本発明の第2の実施形態における図9のスクランブル通信システムのデータ送信部を示すブロック図。

【図16】本発明の第2の実施形態における図9のスクランブル通信システムのデータ受信部を示すブロック図。

【図17】本発明の第3の実施形態における情報配送システムを示すブロック図。

【図18】本発明の第3の実施形態における図17の情報配送システムの中継装置を示すブロック図。

【図19】本発明の第3の実施形態における図18の中継装置の転送処理部を示すブロック図。

【図20】本発明のスクランブル通信を適用した電子新聞配送システムを示すブロック図。

【図21】本発明のスクランブル通信を適用した情報ネットワークシステムを示すブロック図。

【符号の説明】

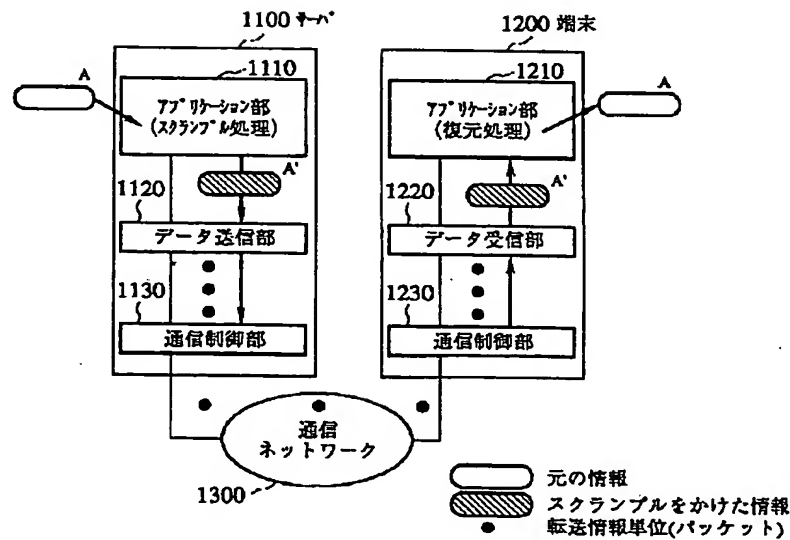
- 10 アプリケーション
- 20 プロトコル処理部
- 30 通信ネットワーク
- 40 プロトコル処理部

50 アプリケーション
 100 サーバ
 110 アプリケーション部
 120 データ送信部
 121 パケット分割部
 122 スランブルキー格納部
 123 スランブル処理部
 124 空き時間監視部
 125 パケット組み立て部
 130 通信制御部
 200 端末
 210 アプリケーション部
 220 データ受信部
 221 復号部
 222 アセンブルキー格納部
 223 データ結合部
 224 空き時間監視部
 225 パケット分解部
 230 通信制御部
 240 復元鍵

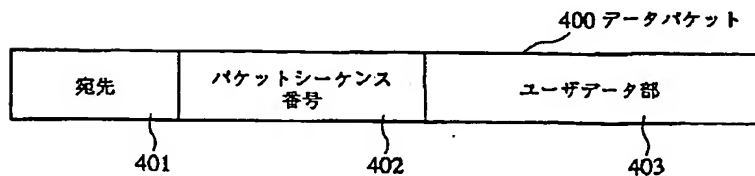
*300 通信ネットワーク
 300-1~300-n 中継装置
 310 転送処理部
 311 宛先変換テーブル格納部
 312 転送データバッファ
 313 転送データ制御部
 320 中継受信部
 321 データ受信部
 322 通信制御部
 10 330 中継送信部
 331 データ送信部
 332 通信制御部
 400 データパケット
 401 宛先
 402 パケットシーケンス番号
 403 ユーザデータ部
 500 配送センタ
 600 販売所
 700a~700f ネットワーク

*20

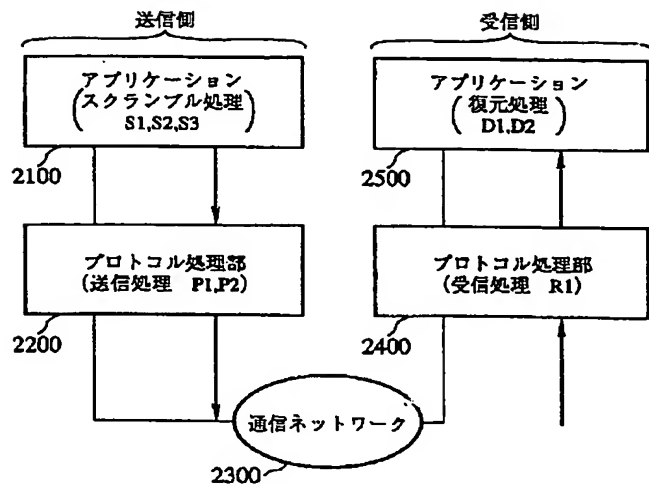
【図1】



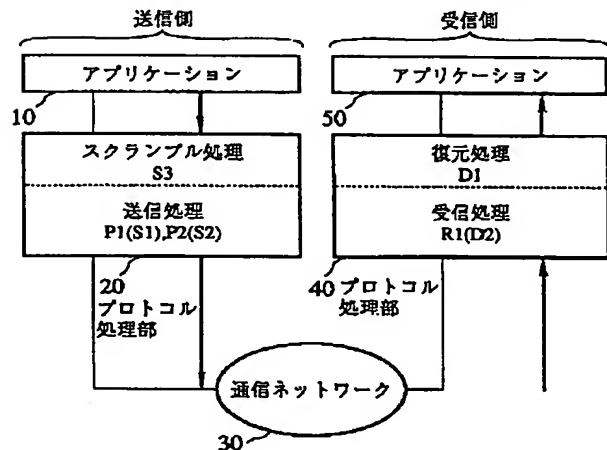
【図11】



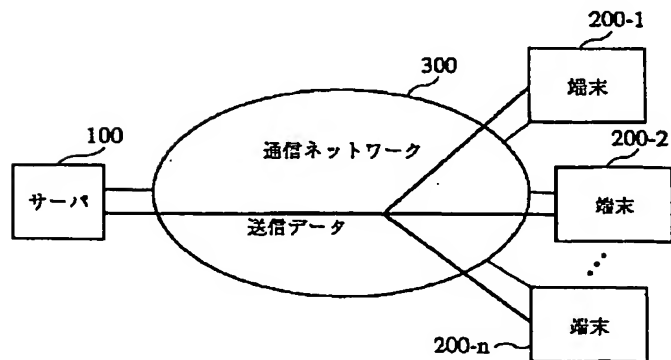
【図2】



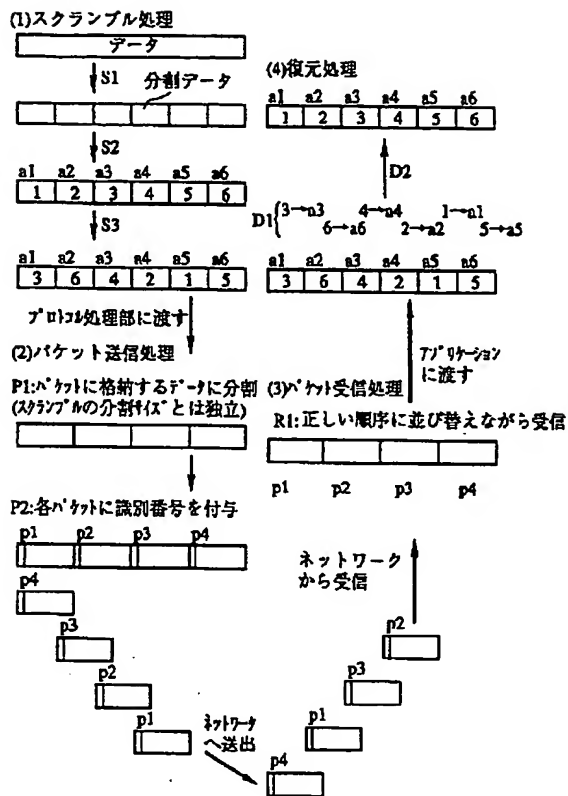
【図4】



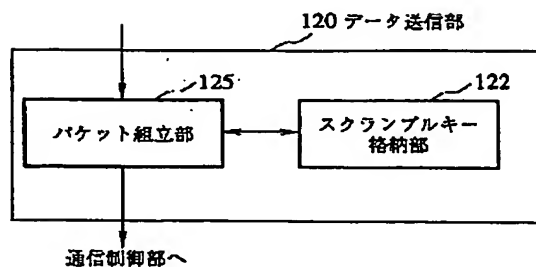
【図8】



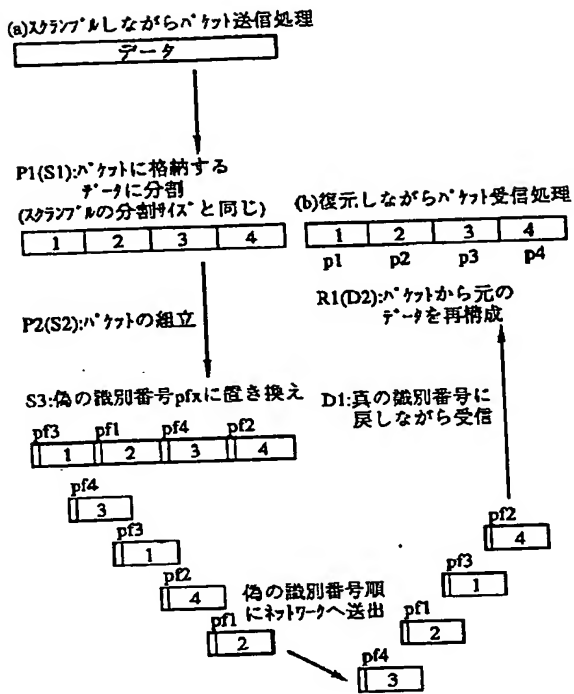
【図3】



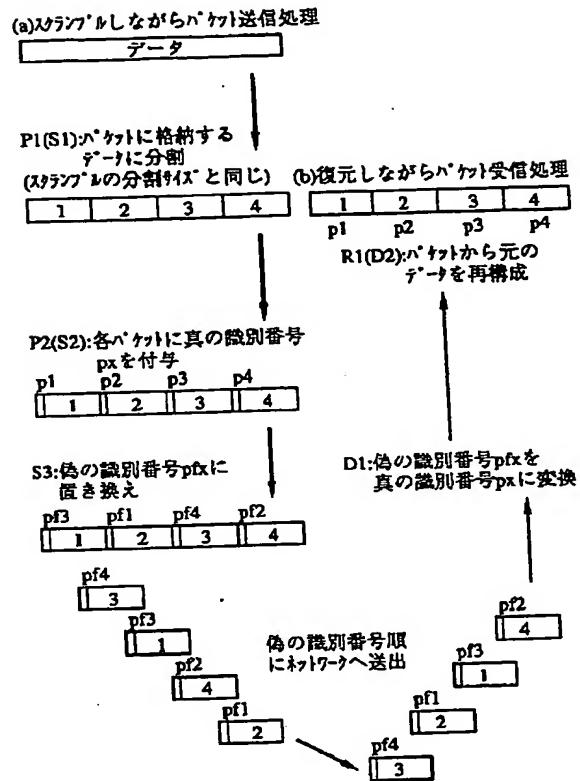
【図15】



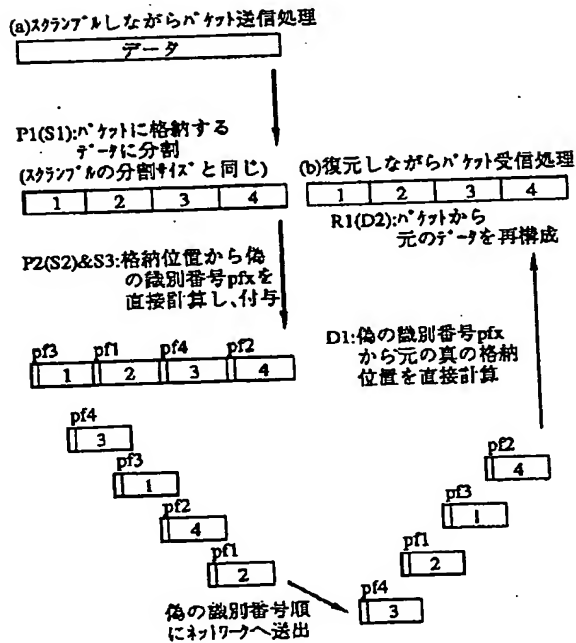
【図5】



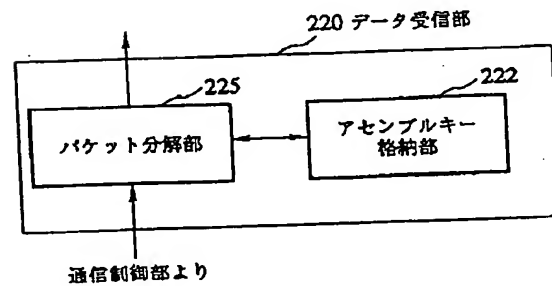
【図6】



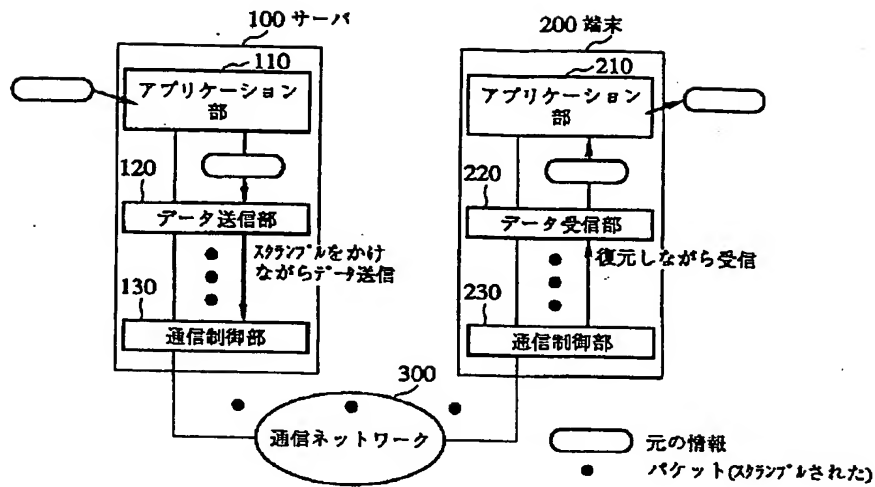
【図7】



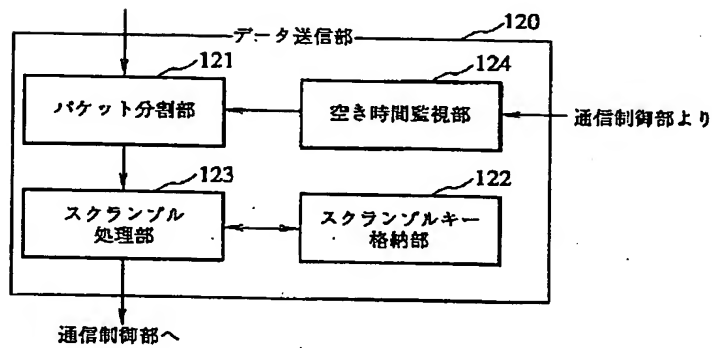
【図16】



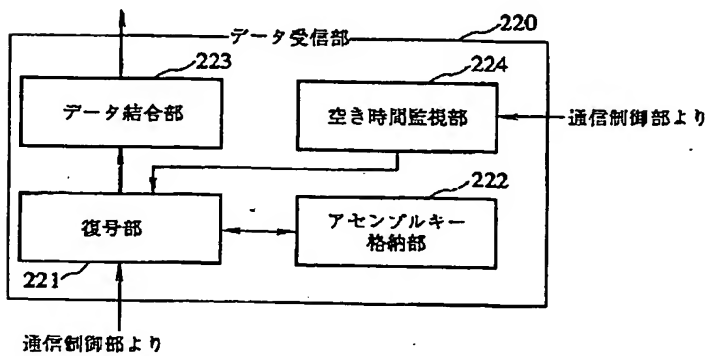
【図9】



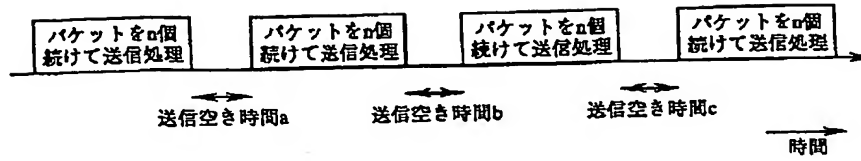
【図10】



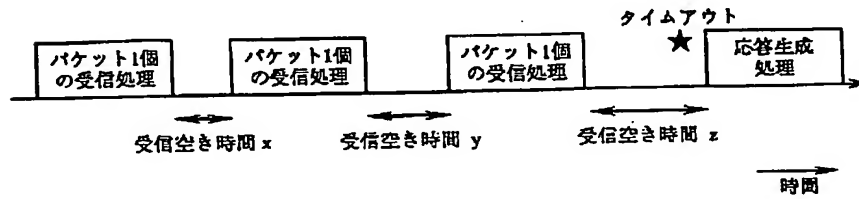
【図12】



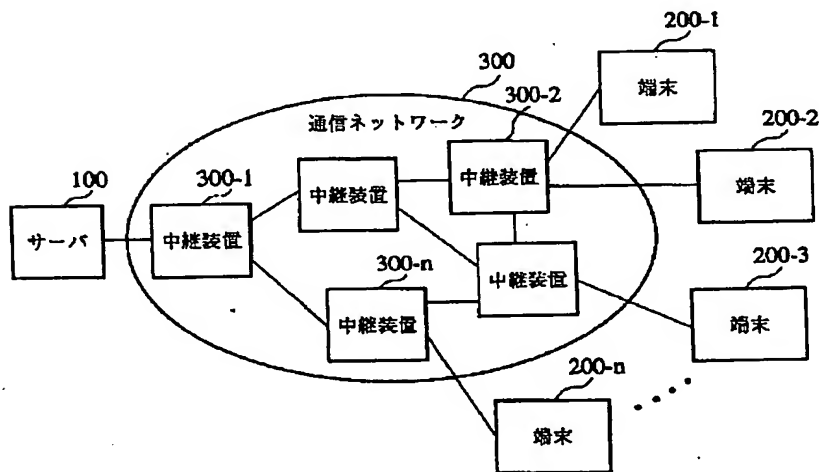
【図13】



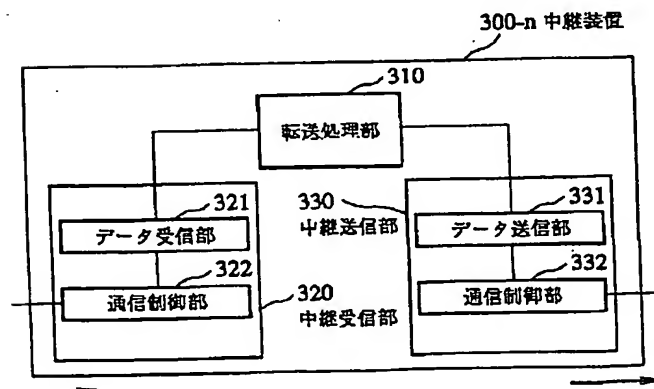
【図14】



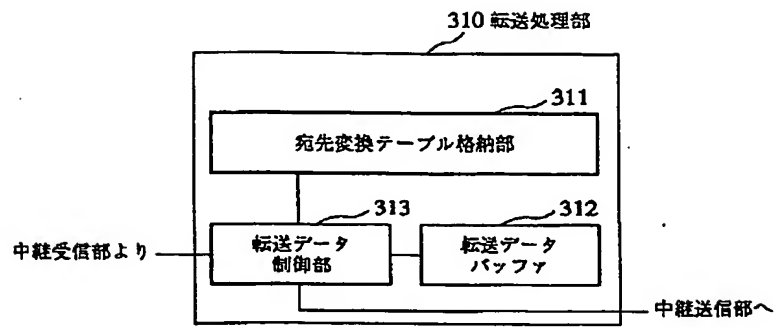
【図17】



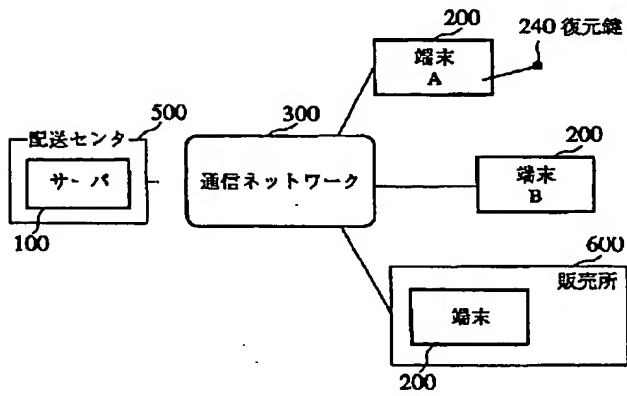
【図18】



【図19】



【図20】



【図21】

